UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/692,265 | 10/23/2003 | John R. Lambert | MS1-1714US | 1569 |

22801 7590 07/09/2008

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

| EXAMINER | |
|---|---|
| DUNN, DARRIN D | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2121 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 07/09/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/692,265 | LAMBERT ET AL. | |
| | Examiner | Art Unit | |
| | DARRIN DUNN | 2121 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *06 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) *18 and 37* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17,19-36 and 38-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This Office Action is responsive to the communication filed on 03/06/2008.

2. Claims 1-17, 19-36, and 38-41 are pending.

### *Claim Rejections - 35 USC § 102*

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-4, 8-17, 19-23, 27-36, and 38 – 41are rejected under 35 U.S.C. 102(e) as being anticipated by Scarfe et al. (USPN 2004/0103021)

5. As per claims 1 and 39, Scarfe et al. teaches a method for investigating messages passed in a message-passing environment, comprising:

collecting a plurality of messages –([0010] e.g., log) from at least one participant –([0030], e.g. IP addresses) in the message-passing environment -([FIG 1]) , wherein each message has a first piece describing transfer information – ([0010] e.g. source/destination IP address) and a second piece describing an operation being performed in the message – ([COL 8], [Table 1] e.g., No. packets sent by IP address, i.e., operation)

assembling the messages into at least one message sequence- ([0030-31], [FIG 8], [0055] e.g., applicant's instant specification discusses a "message sequence" as any grouping of one or more messages. Here, Scarfe et al. teaches categorizing (e.g., grouping) network traffic into IP

address. The messages are accumulated over specific time periods and categorized (e.g., grouped : classification of IP addresses using time periods) according to the IP address. It is interpreted that messages per IP source are grouped together for analysis and subsequently assigned a cluster, such as cluster G. For example, as in a case of an attack from an IP source over successive period within 24 hrs, it would be possible to assign this activity to a cluster)

analyzing said at least one message sequence to extract information –([FIG 8], [0031 e.g., clusters characterizing the data, [0076]) regarding at least the one participant (e.g., IP address) in the message passing environment ([FIG 1]), wherein the analyzing comprises comparing at least one message sequence –([FIG 8-cluster Z] e.g., first grouping of messages with a time period for an IP address corresponding to a cluster) with a reference message sequence – ([FIG 8- cluster F] e.g., second cluster corresponding to messages within a time period for the same IP address. Paragraph [0031] discusses that changes in cluster classification between successive time periods provides information about the behavior of an IP address. In effect, it is interpreted that categorized messages are compared using cluster assignments), the reference message sequence comprises a sequence that reflects an error- free operation in the message passing environment ([COL 9 – element N] e.g., cluster assignment corresponding to categorized IP messages for that time period, where cluster N is identified as normal. 'Reference' is interpreted to mean that a comparison takes place between subsequent message groupings)

outputting the information –([FIG 8] e.g., cluster groups and subsequent changes over 24 hrs)

5. As per claim 2, Scarfe et al. teaches the method according to claim 1, wherein the message-passing environment is a network environment including plural participants coupled together via a network ([FIG 1], [FIG 8] e.g., Internet traffic and IP addresses of participants)

6. As per claim 3, Scarfe et al. teaches the method according to claim 2, wherein the network uses an Internet Protocol – ([0010] e.g., TCP) to transmit messages between participants.

7. As per claim 4, Scarfe et al. teaches the method according to claim 2, wherein the messages express the information in one of a plurality of message formats – ([0010] e.g., FTP, Telnet, HTTP, ICMP)

8. As per claim 8, Scarfe et al. teaches the method according to claim 1, wherein the message-passing environment is a machine or system including plural interacting components that function as message participants ([FIG 8])

9. As per claim 9, Scarfe et al. teaches the method according to claim 1, wherein the message-passing environment is a software program ([FIG 4]) including plural interacting software modules that function as message participants.

10. As per claim 10, Scarfe et al. teaches the method according to claim 1, further comprising, after the collecting, converting identifying information pertaining to said at least one participant into an indication of a role played – ([0004], [FIG 8] e.g., attacks and sources of attacks are identified) by the participant in the message-passing environment.

11. As per claim 11, Scarfe et al. teaches the method according to claim 1, wherein the assembling comprises combining multiple message traces into said at least one message sequence ([0010] e.g., messages are analyzed for time of arrival (e.g., tracing), each message

trace pertaining to one or more messages transmitted by/and or received by a participant ([0010] e.g., number of messages sent or received)

12. As per claim 12, Scarfe et al. teaches the method according to claim 1 wherein the assembling comprises assembling plural message sequences – [0010], [FIG 8 e.g., categorization of messages for multiple IP addresses (e.g., plurality of message sequences) and the analyzing comprises analyzing the plural message sequences ([FIG 8] e.g., 24 hr period analysis)

13. As per claim 13,, Scarfe et al. teaches the method according to claim 1, wherein the analyzing involves performing cluster analysis to group said at least one message sequence into at least one cluster ([FIG 8 –cluster G], [0031])

14. As per claim 14, Scarfe et al. teaches the method according to claim 13, wherein the cluster analysis comprises:

forming a data matrix based on information in said at least one message sequence ([Table 1-matrix], [0082], [0055-56] e.g., information is based upon number of packets sent); and

forming said at least one cluster based on the data matrix ([0055])

15. As per claim 15, Scarfe et al. teaches the method according to claim 14, wherein the forming of the data matrix involves extracting features – ([0056-57] e.g., mean packet length)

16. As per claim 16, Scarfe et al. teaches the method according to claim 14, wherein forming the data matrix –([Table 1], [0118]) involves forming a similarity measure – ([0083] e.g., factors) which measures the difference between said at least one message sequence and another message sequence (e.g., interpreted that factors are applied to a messages, first message sequence, received from an IP address for a time period. Based on the analysis of the factors corresponding

to a time period, the IP address is assigned to a cluster. For a second time period encompassing messages, i.e., another message sequence, the same factors are applied.)

17. As per claim 17, Scarfe et al. teaches the method according to claim 13, wherein the analyzing involves identifying results of the cluster analysis that may warrant further investigation ([0109] e.g., detecting changes in behavior )

18. As per claim 19, Scarfe et al. teaches a computer readable medium including machine readable instructions for implementing the collecting, assembling, analyzing, and outputting recited in claim 1 ([FIG 6])

19. As per claim 20, Scarfe et .al teaches an apparatus for investigating messages passed in a message-passing environment (FIG 1] comprising:

message aggregation logic - ([0031-identifying means]) configured to collect a plurality of messages (e.g., IP packets) from at least one participant (e.g., IP address) in the message-passing environment –(FIG 1), and assembling the messages into at least one message sequence-([0030-31], [FIG 8], [0055] e.g., applicant's instant specification discusses a "message sequence" as any grouping of one or more messages. Here, Scarfe et al. teaches categorizing (e.g., grouping) network traffic into IP address. The messages are accumulated over specific time periods and categorized (e.g., grouped) according to the IP address. It is interpreted that messages per IP source are grouped together for analysis and subsequently assigned a cluster, such as cluster G. For example, as in a case of an attack from an IP source over 24 hrs, it would be possible to assign this activity to a cluster)

analysis logic configured to analyze said at least one message sequence from the message passing environment to extract information regarding at least the one participant in the message

–([FIG 8], [0031 e.g., clusters characterizing the data, [0076]) regarding at least the one participant (e.g., IP address) in the message passing environment ([FIG 1]), wherein the analysis logic is further configured to compare said at least one message sequence –([FIG 8-cluster Z] e.g., first grouping of messages with a time period for an IP address corresponding to a cluster) with a reference message sequence – ([FIG 8- cluster F] e.g., second cluster corresponding to messages within a time period for the same IP address. Paragraph [0031] discusses that changes in cluster classification between successive time periods provides information about the behavior of an IP address. In effect, it is interpreted that categorized messages are compared using cluster assignments), the reference message sequence comprises a sequence that reflects an error- free operation in the message passing environment ([COL 9 – element N] e.g., cluster assignment corresponding to categorized IP messages for that time period, where cluster N is identified as normal)

outputting the information –([FIG 8] e.g., cluster groups and subsequent changes over 24 hrs)

21])

20. As per claim 21, Scarfe et al. teaches apparatus according to claim 20, wherein the message-passing environment is a network environment including plural participants coupled together via a network ([FIG 1])

21. As per claim 22, Scarfe et al teaches the apparatus according to claim 21, wherein the network uses an Internet Protocol to transmit messages between participants ([0010] e.g., TCP)

22. As per claim 23, Scarfe et al. teaches the method according to claim 2, wherein the messages express the information in one of a plurality of message formats – ([0010] e.g., FTP, Telnet, HTTP, ICMP)

23. As per claim 27, Scarfe et al. teaches the apparatus according to claim 20, wherein the message-passing environment is a machine or system including plural interacting components that function as message participants ([FIG 1])

24. As per claim 28, Scarfe et al. teaches the apparatus according to claim 20, wherein the message-passing environment is a software program including plural interacting software modules that function as message participants ([FIG. 3])

25. As per claim 29, Scarfe et al. teaches the apparatus according to claim 20, wherein the message aggregation logic is further configured to convert identifying information pertaining to said at least one participant into an indication of a role played ([0004], [FIG 8] e.g., attacks and sources of attacks are identified)

26. As per claim 30, Scarfe et al. teaches the method according to claim 1, wherein the assembling comprises combining multiple message traces into said at least one message sequence ([0010] e.g., messages are analyzed for time of arrival (e.g., tracing), each message trace pertaining to one or more messages transmitted by/and or received by a participant ([0010] e.g., number of messages sent or received)

27. As per claim 31, Scarfe et al. teaches the apparatus according to claim 20 wherein the message aggregation logic is configured to assemble plural message sequences [0010], [FIG 8 e.g., categorization of messages for multiple IP addresses (e.g., plurality of message sequences

analysis logic is further configured to analyze the plural message sequences ([FIG 8] e.g., 24 hr period analysis)

28. As per claim 32, Scarfe et al. teaches the apparatus according to claim 20, wherein the analysis logic is configured to perform cluster analysis to group said at least one message sequence into at least one cluster FIG 8 –cluster G], [0031])

29. As per claim 33, Scarfe et al. teaches the apparatus according to claim 32, wherein, in performing the cluster analysis, the analysis logic is further configured to:

form a data matrix based on information in said at least one message sequence ([0082], [0055-56], [Table 1- matrix] e.g., information is based upon number of packets sent)

form said at least one cluster based on the data matrix ([0055])

30. As per claim 34, Scarfe et al. teaches the method according to claim 14, wherein the forming of the data matrix involves extracting features – ([0056-57] e.g., mean packet length)

31. As per claim 35, Scarfe et al. teaches the method according to claim 14, wherein forming the data matrix –([Table 1], [0118]) involves forming a similarity measure – ([0083] e.g., factors) which measures the difference between said at least one message sequence and another message sequence (e.g., interpreted that factors are applied to a messages, first message sequence, received from an IP address for a time period. Based on the analysis of the factors corresponding to a time period, the IP address is assigned to a cluster. For a second time period encompassing messages, i.e., another message sequence, the same factors are applied.)

32. As per claim 36, Scarfe et al. teaches the method according to claim 13, wherein the analyzing involves identifying results of the cluster analysis that may warrant further investigation ([0109] e.g., detecting changes in behavior )

33. As per claim 38, Scarfe et al. teaches a computer readable medium including machine readable instructions for implementing the collecting, assembling, analyzing, and outputting recited in claim 1 ([FIG 6])

29. As per claims 40 and 41, Scarfe et al. teaches a method according to claim 1, wherein the reference message sequence is a sequence that reflects known failure conditions within the message passing environment ([0109] e.g., cluster pairing reflect device failure. It is interpreted that messages pertaining to a failure are categorized and assigned a cluster)

***Claim Rejections - 35 USC § 103***

30. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

31. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

32. Claims 5-7 and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scarfe et al. (USPN 2004/0103021) in view of Greifeneder et al. (USPN 20040243349)

33. As per claims 5 and 24, Scarfe et al. teaches an apparatus according to claims 1 and 21 (respectively) but does not teach where the messages include information expressed in a markup language. Greifeneder et al teaches that network traffic may comprise documents including XML, GIF, and JPG communicated using network protocols, including but not limited to SOAP ([0064], [0019])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Scarfe et al. to include xml based messages. Scarfe et al. teaches collecting information pertaining to network traffic for classification and analysis. Greifeneder et al. teaches a method and system for monitoring and the analysis of networked systems. Xml base messages are a common format utilized in network communication. Since xml messages include data about data, it would have been obvious to group and analyze such messages for pertinent information about the behavior of a sender/receiver within a network.

34. As per claims 6 and 25, Greifeneder et al. teaches wherein the markup language is xml ([0064] e.g. XML)

35. As per claims 7 and 26, Greifeneder et al. teaches wherein the network uses Simple Object Access Protocol to transmit messages between participants ([0019] e.g. SOAP)

***Conclusion***

36. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

20040015719

20040054505

20040098617

20080104060

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARRIN DUNN whose telephone number is (571)270-1645. The examiner can normally be reached on EST:M-R(8:00-5:00) 9/5/4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert DeCady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DD
07/01/08

/Albert DeCady/
Supervisory Patent Examiner
Art Unit 2121